SPARK Matrix™

Security & Risk Management

SPARK Matrix™: User Authentication, 2021

Market Insights, Competitive Evaluation, and Vendor Rankings

October 2021

Table of Contents

Executive Overview

This research service includes a detailed analysis of the user authentication solution, market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides a comprehensive competition analysis and ranking of the leading user authentication vendors in the form of the SPARK Matrix. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors' capabilities, competitive differentiation, and market position.

Key Research Findings

Followings are the key research findings:

The vendors of user authentication offerings continue to strengthen their value proposition by significantly investing in enhancing capabilities such as onboarding, authorization support, analytics, audit and reporting, single sign-on (SSO). Vendors are focusing on cloud-first approach/cloud-native containerization supporting both on-prem and customer-managed cloud, improving mobile security, contextual signals, and model improvements. Leading User Authentication vendors are constantly augmenting their solution capabilities with native AI to continuously analyze user behavior to discover security breaches, monitor and protect networks, endpoints, active directories, applications, and data from various types of threats.

Key Market Drivers and Technology Trends:

- User authentication solutions are evolving, becoming more robust and gaining traction with forward-thinking solution providers, specifically when user authentication vendors are expanding into multiple sectors by introducing new capabilities to monitor privileged users, meet different needs and requirements of organizations, and enable a robust response to advanced threats and enhance user experience.
- With the massive proliferation of unsecured BYOD, WYOD, and IoT devices across enterprises resulting increase in threats and data loss, there is an increasing focus on ensuring secure user access and protecting the privileged organizational resources.
- The demand for user authentication solutions is increasing as organizations are providing access to employees as well as other persons outside the organization’s security perimeter, including contractors and remote vendors to the organizational network, applications, and databases. User authentication

applications allow organizations to authenticate employees, remote vendors, and contractors in real-time to stop network security breaches and data losses.

- The other market drivers for the growth of the user authentication market include continued investments in digital transformation projects leading to increased adoption of cloud and hybrid infrastructures, increased use of mobile and personal devices, remote working, and growing complexities of the global regulatory environment.

- Driven by the growing market opportunity, vendors are focusing on offering robust user authentication platforms to secure organizations' networks, servers, data, websites, and applications from anonymous users. These platforms offer capabilities such as onboarding, authorization support, analytics, auditing and reporting, and SSO (Single Sign-On) for managing/facilitating user authentication in a holistic manner. With the continuous evolution and increasing sophistication of user threats, vendors are rapidly adopting AI, ML, and new robust techniques to offer enhanced user authentication capabilities. Vendors are leveraging AI, ML, and other technologies to offer robust detection capabilities, automate API discovery, deep traffic visibility, reporting, threat detection, and cyberattack prevention.

- COVID-19-induced disrupted business scenarios, growth in remote working, and increased risk is driving significant investments in user authentication solutions. Organizations are focusing on providing continuous, dynamic, and real-time secured access to the users.

- The emergence of stringent data privacy regulations such as GDPR, CCPA, and others is forcing businesses to adopt advanced security and compliance solutions to improve their defense strategies and comply with stringent regulatory requirements.

- Many leading user authentication platform providers are offering essential elements of modern security such as cloud and network security and fraud prevention activities. Also, vendors are offering an advanced form of multi-factor authentication (MFA), Adaptive Authentication (Risk-Based Authentication), to select the appropriate authentication method based on a user's risk profile and update the type of authorization factors.

- Organizations' interest in passwordless authentication is increasing, as it provides secured, passwordless access to applications or IT systems, allowing organizations to enhance user experience and increase security and simplify IT operations.

- Organizations are looking for vendors offering continuous, real-time, and dynamic authentication to secure their networks and protect them from advanced threats. Additionally, the vendors are providing robust features, supporting diverse use cases, and have a presence in different verticals, including banking & financial services, retail, IT & Telecom, and such others.

Competition Dynamics & Trends:

- This study includes analysis of key vendors, including Boloro, Broadcom, Cisco, Deepnet Security, Entrust, FacePhi Biometria, FaceTec, ForgeRock, Forticode, HID Global, IBM, ID R&D, ImageWare Systems, Intensity Analytics, i-Sprint Innovations, KOBIL GmbH, Microsoft, Nexus, Nuance, NuData Security, Okta, OneSpan, Ping Identity, Prove, PointSharp, RSA, SecureAuth, SecureEnvoy, Thales, Unisys, and Veridium.
- Cisco, Entrust, ForgeRock, HID Global, IBM, NuData Security, OneSpan, Ping Identity, Prove, and Thales are the top performers in the global User Authentication market and have been positioned as the top technology leaders in the 2021 SPARK Matrix analysis of the user authentication market.
- Broadcom, i-Sprint Innovations, Microsoft, Nuance, Okta, RSA, SecureAuth, and Unisys have been positioned amongst the primary challengers. The other key vendors captured in the 2021 SPARK Matrix include ImageWare Systems, Veridium, ID R&D, Nexus, FaceTec, Intensity Analytics, Forticode, Boloro, SecureEnvoy, PointSharp, and Deepnet Security.

Market Overview and Technology Trends

Quadrant Knowledge Solutions defines a user authentication solution as “software that verifies the identity of a user attempting to access a network or a resource by exchanging credentials in the form of OTPs, hardware tokens, multi-factor authentication (MFA). The authentication process works by matching a user’s access request with a set of identifying credentials in various formats, including those mentioned above.

Organizations have been using DHCP (Dynamic Host Configuration Protocol) to authenticate devices on their networks so that they can access network services such as DNS, NTP, and any UDP or TCP-based communication protocol. However, authentication issues persist. The situation is aggravated by various factors such as the rise in digital transformation, COVID-19 pandemic-driven rise in remote work, and the consequent increase in the number of personal and unsecured devices accessing secure organizational networks that have added new vulnerabilities to organizations’ threat landscape. These factors are driving the rise in demand for user authentication solutions, as these solutions can enhance the access security of employees, partners, and customers to electronic or digital assets. User authentication solution help organizations identify, authenticate, and authorize users in real-time. They also allow organizations to verify the identities of the users trying to access the organizational network and resources. User authentication technology leverages important elements of modern security, including cloud and network security and fraud prevention activities.

User authentication is a robust process that allows organizations to identify, authenticate, and authorize users connected to the network resources. It provides secured access to the authorized users to the privileged resources, blocks the unauthorized users in real-time, and helps stop system damages, account takeovers, new account takeovers, information theft, fraudulent transactions, and such other crimes. Additionally, user authentication helps manage user identity and access across cloud, mobile, and on-prem environments. User authentication allows organizations to enhance network, application and data security, reduce password threats and fraud, and maintain GDPR, PSD2, and other regulatory compliance.

User authentication involves various authentication methods such as password-based authentication (includes the password for each server and admin maintains each user name and passwords), and multi-factor authentication (includes two or more verification methods to provide secured access to resources like applications, online accounts, or a VPN). Certificate-based authentication includes digital certificates to detect user and device before providing access to resources, networks, and applications. Biometric authentication includes an individual’s unique biological traits to authenticate users’ access to physical and digital resources. Token-based

authentication involves encrypted security tokens to authenticate users and provide secured access to the websites, apps, or any resources without re-entering credentials each time. Adaptive authentication (risk-based authentication) offers an extra layer of multi-factor authentication protection based on the risk and access granted by the security administrator to manage user access. Additionally, adaptive authentication allows organizations to enhance data security, improve productivity, prevent fraud, minimize IT costs, and integrate APIs .

A user authentication platform provides key capabilities, including onboarding, authorization support, analytics, audit and reporting, and Single Sign-On (SSO), enabling organizations to reduce costs and improve security. User authentication platform enables organizations to provide the right access to the applications, files, and other privileged resources at the right time by verifying the users. In addition, user authentication solutions can reduce the possibilities of breaches, as organizations can leverage the solutions to provide secure access from devices outside the organization's security perimeter.

Following are the key capabilities of a user authentication solution:

- **Onboarding-** A user authentication solution allows organizations to authenticate and authorize users and device onboarding with technologies like authenticators, mobile authentication, mobile ID proofing, multi-factor authentication (MFA), passwordless login, safeguarding user VPNs, single-sign-on, and credential issuance. User Authentication provides customers with a liberating mobile onboarding experience, secures digital onboarding by verifying the user's 3D liveness with a previously uploaded video-selfie and comparing the user's face with their Photo ID, OCRs the ID Text, and analyzes previous enrolled FaceMaps to check for duplicates. User authentication allows organizations to securely build up digital onboarding journeys, authenticate end-users in real-time, and control the entire user lifecycle from onboarding to archiving.

- **Authorization Support-** A user authentication solution enables automatic and continuous authorization of a user when they request or try to access privileged data and applications. User authentication offers robust user authorization support and password management capability. A user authentication platform leverages multi-factor authentication (MFA) techniques and improves security by removing risky password management practices. MFA uses various credentials such as passwords, messages, digital access cards, and biometric verification to authenticate users. It helps to detect and respond to high-risk logins and easily reset passwords. User Authentication may also support adaptive authentication based on risk and contextual information (location, time-of-day, IP address, device type, etc.) It provides enhanced security and controls access to resources by automatically blocking risky users in real-time.

- **Analytics–** A user authentication platform includes analytics to detect and manage dormant and orphaned accounts, inappropriate entitlements, identify and prevent fraud and automated threats in real-time, and meet organizational security requirements. User authentication leverages real-time risk profiling technology based on data analytics. User authentication analytics allows analysis of the risk associated with the user's login and post-login behaviors and prompts for step-up authentication in the circumstances deemed high-risk or in violation of organizational regulations. User authentication analytics provides comprehensive information on how entities use their access, their roles and responsibilities, and job duties. It also provides information on application and data usage. User authentication solutions can analyze users' access and detect anomalies in users' functions and data usage for enhanced security. Anomaly detection enables organizations to detect irregularities such as active accounts of retired workers or anomalous usage patterns of a particular workforce/ customer/ partner. Additionally, it helps identify threats and suspicious user behavior, investigate events, analyze trends, facilitate access log monitoring and alerting/reporting capabilities, and improve compliance and governance.

- **Audit and Reporting-** User authentication solutions also allow organizations to easily audit users' and suppliers' access and provide information regarding their activities. With audit and reporting capability, organizations can spot and prevent any fraudulent activity in real-time. User authentication provides behavioral data on the dashboard to analyze users, capture and stop suspicious user access. User authentication leverages a reporting module that provides role-based access to view, edit, and create reports and supports all authentication technologies and existing SIEM, SOAR, SSO, IDaaS, and CIAM solutions with standard reporting. A user authentication solution provides flexible user roles and comprehensive reporting that includes important insights into users' security profiles. Additionally, organizations can keep track of user activities in real-time, and lastly, can create comprehensive reports for audit trail requirements with the help of the user authentication solution.

- **Single Sign On (SSO)-** A user authentication solution offers identity federation through the Single Sign-On (SSO) technique, which enables users to access multiple business applications and services using a single set of login credentials from any device. SSO enables users to authenticate themselves once and then grants them access to all the software, systems, and data they need without logging in to each of those individually. SSO enhances the user experience by making the login process quick and simple and eliminating the need to remember different passwords for different applications. It offers increased productivity, IT monitoring & management, and security control by enabling/disabling user access to multiple

applications and resources with a single security token. It also reduces the risk of lost, weak, or forgotten passwords. SSO provides end-to-end access management by approving or rejecting end-users requests and access to all services from a single location with a single click by leveraging a single pane of glass.

Factors Influencing Market Development and Growth

The following dominant technology and market developments are influencing the growth of the overall global user authentication market:

Cloud and Hybrid IT Infrastructures is Driving the Adoption of User Authentication Solutions

The growing adoption of multi-cloud and hybrid IT environments is considerably increasing the enterprise attack surface. As a consequence, organizations are looking at enhancing their threat defense measures to address the ever-growing security risks, internal threats, external malware, and compliance requirements associated with hybrid IT infrastructure. With applications and infrastructure moving to multi-cloud and hybrid locations, organizations are looking for measures to protect these resources from attacks and at the same time make sure that authentic users and get uninterrupted and seamless access. Organizations are also required to manage multiple devices and access points to secure access to cloud applications and resources. Therefore, enterprises are embracing user authentication solutions for comprehensive authentication and authorization of users prior to access. User authentication solutions provide direct and secure access to public cloud applications and resources. Hence, they are becoming a popular security measure for the hybrid IT environment. With Single Sign-On (SSO) and MFA features, etc., user authentication solutions eliminate the cumbersome manual password management process, enable high security, and ensure a seamless and enhanced customer experience.

Robust User Authentication solutions for boundaryless security

With organizations operating from multiple locations worldwide, applications and resources need to be accessible from anywhere. Organizations are increasingly using cloud-based applications and adopting hybrid infrastructures to tackle this issue. With organizations becoming boundaryless, they often face challenges related to data and user security. Moreover, with an increasing number of employees, customers, and partners accessing the company's applications and resources from different devices, unifying access policies across all device platforms, including desktops, laptops, smartphones, and tablets, is crucial. Organizations are focusing

on investing in security solutions that can continuously authenticate, authorize users in real-time, and secure organizational networks and resources. With user authentication solutions, organizations can detect, authenticate, and authorize users connected to the network resources in real-time. Additionally, user authentication solutions provide a fine-grained and contextual access policy, allowing secure connection based on who can connect from which devices and to what resources. In addition, user authentication solutions support all organizations' applications, be it cloud-based or on-prem, and unify access policy across apps and devices. Thus, user authentication solutions ensure that all the required resources are accessed by the right person and secured regardless of where they are stored.

Increasingly Complex Global Regulations and Compliance Requirements landscape

Numerous compliance frameworks, such as NIST, FISMA, HIPAA, PCI-DSS, and others, are significantly impacting the overall enterprise security strategies across industry verticals and geographical regions. While compliance with global, country, and industry regulations can help improve an organization’s security posture, non-compliance can result in a higher risk of information theft, fines, liabilities, negative publicity, and more.

Additionally, the EU’s General Data Protection Regulation (GDPR) has ushered in a global standard in data privacy with extensive specifications and potential penalties. GDPR kept the businesses busy restructuring their policies to comply and started a wave of privacy regulations across the globe. In line with GDPR, California has introduced its data privacy law-CCPA (California Consumer Privacy Act). CCPA holds businesses in California accountable for how they collect, share and secure personal consumer data. Additionally, 11 states of the US have passed legislation strengthening their data privacy laws. Other countries like Australia and Canada also followed suit in updating their consumer data privacy laws. Businesses should expect more such regulations in the future, as the rest of the world also responds to the increasing public pressure against data breaches and exfiltration.

A user authentication solution can significantly help organizations to authenticate and authorize users connected to the network resources and improve overall security and compliance requirements. The solution secures access to IT resources without relying on protocols, networks, or locations. Additionally, it allows organizations to manage user identity and access across cloud, mobile, and on-prem environments in real-time, enhance network, application and data security, reduce password threats and fraud, and maintain GDPR, PSD2, and other regulatory compliance.

COVID 19-induced spike in remote working driving the surge in demand for robust user authentication solutions.

The coronavirus pandemic has impacted the world's economy and driven the global workforce indoors. However, this remote working is also creating its fair share of problems, the biggest one being security. With the global organizations allowing working from home, employees/ vendors/ contractors are using their own devices and personal unsecured networks to access sensitive organizational resources. Such usage is providing hackers with greater chances of gaining access to this sensitive data. Driven by all these challenges, user authentication solutions are getting a lot of traction from organizations as they can provide secure access to applications and privileged data in the cloud and on-prem. With user authentication solutions, organizations can authenticate users working from different locations from the device of their choice and provide access to only those authenticated entities. User authentication solutions provide access to authenticated users and block unauthorized users in real-time. The solutions offer secure access to critical applications and resources while enforcing granular continuous and adaptive authentication. The current need for remote onboarding of employees and customers is another factor driving the importance of identity proofing and verification capabilities in user authentication solutions. User authentication solutions provide flexible and modern authentication methods for cloud-based security to respond to the risks of remote and BYOD users.

AI, ML and Advance Analytics intelligently augment user authentication solutions for advanced security

Artificial intelligence and machine learning technologies are becoming a driving force for vendors to protect and monitor networks, endpoints, active directories, applications, and data from malicious attacks. Thus, AI/ML techniques are acting as significant constituents in helping organizations optimize threat hunting and prevent cybercrimes.

Owing to the enormous benefits of user authentication techniques, organizations are increasingly adopting user authentication solutions to secure organizational network and resources. User authentication solutions enable highly secure identity and access across cloud, mobile, and on premises environment with enhanced user experience. But with IoT, BYOD, remote work, and cloud-based collaboration becoming the norm, there is a drastic increase in the number of endpoints that malicious third-parties can target to gain network access. User authentication solution providers are adopting artificial intelligence, machine learning, and advanced analytics to offer improved security, visibility, to organizations to tackle these challenges. AI/ML is enabling adaptive risk-based MFA for enhanced access security, while advanced analytics, including user and entity behavior analytics, is enabling real-time identity monitoring and analysis. Powered by these emerging technologies, user authentication solutions help organizations restrict access of bad actors and bots, secure users transaction lifecycle, automate API discovery, deep traffic visibility, provide reporting, threat detection, and cyberattack prevention capabilities, maintain user identity integrity, monitor user behavior to identify anomalies, automate authentication for low-risk access situations, and automatically

provide access to the digital resources and detect and prevent data breaches. Additionally, by incorporating AI, ML, and advanced analytics capabilities in their user authentication solution, organizations can immediately detect blind spots, authenticate and authorize users, secure identities, organizational applications, and end-user access to resources, detect threats and respond in real-time. Some user authentication vendors are also investing in AI-driven predictive identity governance capabilities, and a backend AI/ML engine for digital transformation and cyber security revolution.

Passwordless authentication enabling secured and easy logins

Passwordless authentication is becoming more prevalent as many companies have realized that password-based logins are contributing to more cyberattacks, and passwordless authentication can protect them from such incidents and also save time. As compared to passwords, passwordless authentication is more sophisticated, secure, convenient, easy to use, and more complicated to hack. Passwordless Authentication helps organizations enhance user experience and productivity, minimizes security risk, maintenance, and cost, improves employee password hygiene and form conversion rates, stops password theft, protects against brute-force attacks, phishing, and password lists, optimizes organizations' cyber security posture, and provides frictionless signup process. In order to provide a holistic platform, user authentication vendors are combining passwordless authentication with adaptive authentication to provide extra security and privacy. Adaptive authentication leverages ML to detect and develop the patterns from user behavior to address deviation in logins and risky behavior and take necessary actions. Passwordless authentication helps increase workforce productivity by creating a better user experience and providing a better security posture.

Vendors are enabling advanced capabilities for a robust and user-friendly authentication mechanism

As organizations undergo digital transformation, they are looking for more comprehensive security solutions to secure their resources and environment. Vendors are offering advanced capabilities in their user authentication solutions like zero trust, decentralized identity, and continuous authentication for a robust and user-friendly authentication mechanism to fulfill organizational authentication requirements. Decentralized identity provides greater users autonomy, improves privacy, and stimulates digital transformation across enterprises. It allows users to obtain information easily, access digital identification, use blockchain-based cryptography tools to create digital wallets. Zero trust allows organizations to authenticate and authorize users regardless of their location. Zero trust and continuous authentication allow security teams to manage user access and monitor the network environment to gain visibility with their identity solutions. Additionally, it helps to automatically re-authenticate users when an anomaly is detected and provides continuous authentication to improve security posture.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major user authentication solution vendors by evaluating their products, market presence, and value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall user authentication market. This study includes an analysis of the key user authentication vendors, including Boloro, Broadcom, Cisco, Deepnet Security, Entrust, FacePhi Biometria, FaceTec, ForgeRock, Forticode, HID Global, IBM, ID R&D, ImageWare Systems, Intensity Analytics, i-Sprint Innovations, KOBIL GmbH, Microsoft, Nexus, Nuance, NuData Security, Okta, OneSpan, Ping Identity, Prove, PointSharp, RSA, SecureAuth, SecureEnvoy, Thales, Unisys, and Veridium.

Cisco, Entrust, eForgeRock, HID Global, IBM, NuData Security, OneSpan, Ping Identity, Prove, and Thales are the top performers and technology leaders in the global user authentication market. These companies provide a sophisticated and comprehensive technology platform to identify, authenticate, and authorize users connected to the network resources. A user authentication solution provides secured access to the authorized users to the privileged resources, blocks unauthorized users in real-time, and helps stop system damages, account takeovers, new account takeover, information theft, fraudulent transactions, and such other incidents. A user authentication platform helps manage user identity and access across cloud, mobile, and on-prem environments. Additionally, the solution allows organizations to enhance network, application, and data security, reduce password threats and fraud and maintain GDPR, PSD2, and other regulatory compliance.

Cisco offers a comprehensive user authentication product suite, which includes Duo MFA, Duo Access, Duo Beyond, which allows organizations to control user access to the network server and resources. Additionally, Cisco allows organizations to authenticate user identities, gain insights into every device, and implement adaptive controls to secure access to privileged data. Cisco is focusing on increasing the number of customers, geographical presence, different industry verticals, and expanding its use case support.

Entrust offers a cloud-based, holistic identity and access management (IAM) solution to protect financial transactions, manage citizen IDs, and protect digital businesses through authentication, digital certificates, and secured communication. Entrust’s unified IAM portfolio enables a zero-trust approach that provides protection against unauthorized access, data breaches, and other cyberattacks, and fraudulent transactions. Entrust IAM utilizes high-assurance credential-based access, single sign-on (SSO), passwordless access, best-in-class multi-factor authentication (MFA), adaptive risk-based access and authentication, identity proofing, and secure portals to protect identities, payments, access, privileged data.

ForgeRock offers comprehensive identity and access management solutions for secure access to consumers and employees. Additionally, ForgeRock allows organizations to orchestrate, manage, and protect the lifecycle of identities from dynamic access controls risks, governance, APIs, and strong authoritative data in all environments. Additionally, ForgeRock provider of secured access to privileged data and block unauthorized user in real-time.

HID Global offers robust, out-of-the-box solutions to authenticate the users in real-time and protect organizations from various threats. HID Global allows organizations to detect, verify, and authenticate users through its HID Global Authentication Platform,which encompassing Authentication Service, WorkforceID Authentication, HID Approve™, and WorkforceID Digital Credential Manager solutions, Crescendo® Smart Cards and Security Keys, Risk Management Solution and Identity Verification Service. HID Global allows organizations to protect users, websites, and IoT devices. Additionally, the HID Authentication platform includes the award-winning HID Approve™ solution, which combines asymmetric key-based cryptography with push notifications (available as SDK).

IBM provides user authentication through its IBM QRadar, which includes system authentication, radius authentication service server, TACACS authentication, Microsoft active directory, native LDAP server, SAML single sign-on authentication to authenticate users in all environments. Additionally, IBM QRadar automatically updates password policies according to the users existing security standards, allows organizations to customize external authentication providers to allow IBM QRadar to authenticate them without QRadar storing their passwords locally, and configures system authentication, RADIUS authentication, TACACS, active directory authentication, LDAP authentication, and SAML single sign-on authentication.

NuData Security offers behavioral analytics and passive biometric-based NuDetect to detect digital users in real-time. NuDetect analyzes hundreds of devices, locations, passive biometric and behavioral signals with previous user behavior and known patterns to authenticate users. Additionally, NuDetect integrates multi-layered technology to allow organizations to identify valid users and fraud risks in real-time, improve the user experience, and identify unknown users. NuDetect provides continuous and accurate authentication of user behavior in real-time. It also provides intelligent automation detection and allows the identification of threats during the application/registration process to make confident judgments.

OneSpan offers a comprehensive set of powerful, frictionless authentication solutions as well as invisible security features to help organizations reach their security objectives. OneSpan helps organizations to minimize fraud, enhance customer satisfaction, and meet regulatory requirements with its intelligent adaptive authentication, enhance security and authentication by gaining visibility into mobile

security issues with its mobile security suite, improve remote access security with two-factor authentication, prevent fraud and safeguard high-value transactions with user-friendly hardware authentication devices. Additionally, it utilizes authentication servers and API technologies to protect access and transactions and streamline identity management.

Ping Identity offers zero-trust identity-defined security to organizations to enhance protection and engagement across global businesses. The PingOne Cloud Platform allows customers, employees, and partners to securely access the cloud, mobile (web), SaaS, and on-prem applications and APIs. PingOne Cloud Platform offers global authentication, a secure and seamless user interface for business initiatives, and comprehensive APIs for integration and customization. Additionally, it supports standards protocols through OOTB integration with Microsoft O365, social identity providers, token translators, OAUTH/OIDC, SCIM, and more.

Prove offers next-generation Identity-verification software to protect from identity theft and social engineering attacks by identifying individuals with just a phone. Prove provides multi-factor authentication services which leverage deterministic biometric and environmental attributes using machine learning to detect users. Prove enables organizations to passively authenticate users based on their gait (unique walking style) through its GaitAuth technology. Additionally, Prove GaitAuth operates with step-up or continuous authentication routines, as well as a factor in a 2FA/MFA solution. Prove's GaitAuth allows organizations to correctly detect users with accuracy revealing the same as other biometric authentication methods, minimize the explicit authentication methods, continuously authenticate users without interrupting, and differentiate themselves from the competitors with passive authentication.

Thales provides a people-centric User Authentication platform for modern enterprises. Thales offers a cloud-based access management solution, SafeNet Trusted Access which helps control access to both cloud services and business applications through an integrated platform that combines single sign-on, multi-factor authentication, and scenario-based access regulations. Additionally, SafeNet Trusted Access enables organizations to enhance the adoption of cloud services for end-users who face challenges in managing online identities and access security while ensuring comfortability and regulatory compliance. SafeNet Trusted Access automates cloud identity management and enables IT team and users to minimize password hassles while delivering a single pane view of access activities throughout the organizational app to verify that the correct user has access to the right application at the right level of confidence.

KOBIL GmbH provides digital identity and highly secure data technology and enables organizations to provide ongoing identity and mobile security management across all platforms and communication channels. Additionally, it provides secured and trusted

passwordless access and real-time corroboration without any device limitations. KOBIL GmbH includes virtual smart card technology, world-leading PKI technology, hardware extension, multiple security features, and different login methods.

FacePhi Biometria offers SelPhi and SelphID to enhance customer experience and secure data from individuals and organizations. It includes multi-factor biometrics, transaction dashboard, multiplatform solution, provides 24/7 support, and helps users minimize integration time. Some of the key differentiators of FacePhi include on-premise installation, multimodal installation, automatic capture, real-time OCR, certified passive liveness, and tailor-made solutions. Additionally, FacePhi Biometriaprovides a comprehensive and customized solution for digital onboarding, authentication, and security by leveraging different biometric and anti-fraud technologies.

Vendors such as Broadcom, i-Sprint Innovations, Microsoft, Nuance, Okta, RSA, SecureAuth, and Unisys have been positioned amongst the primary challengers. These companies provide comprehensive technology capabilities and are rapidly gaining market traction across industry and geographical regions. These companies are also mindful of the upcoming market trends and have outlined a comprehensive roadmap to tap into future growth opportunities. The other key vendors captured in the 2021 SPARK Matrix include ImageWare Systems, Veridium, ID R&D, Nexus, FaceTec, Intensity Analytics, Forticode, Boloro, SecureEnvoy, PointSharp, and Deepnet Security.

All the vendors captured in the 2021 SPARKMatrix of User Authentication are improving their capabilities to detect and stop risky behavior users in real-time, identify and control violations of corporate policies, monitor and manage data access governance issues, enhance network, application, and data security, and reduce password threats and fraud. Additionally, they help organizations to expand the partnership channels and support diverse use cases. Organizations are consistently looking to enhance user authentication platforms and expand support for multiple deployment options. All the vendors captured in the 2021 SPARKMatrix of User Authentication are improving their capabilities to identify, authenticate, and authorize users connected to the network resources. Vendors continue to augment comprehensive biometric platform with real-time onboarding and authentication flows, transaction control, and result statistics, applying continuous Adaptive Risk and Trust Assessment (CARTA) for Access Management, AI-driven predictive identity governance capabilities, social identity support, voice recognition-based authentication, and security analytics to identify and manage dormant accounts, orphaned accounts, and inappropriate entitlements. Additionally, the companies are focusing on increasing the number of customers, geographical presence, different industry verticals, and expanding use case support. These organizations are

consistently looking to enhance their user authentication platforms and expand support for multiple deployment options.

Key Competitive Factors and Technology Differentiators

Following are the key competitive factors and differentiators for the evaluation of user authentication solutions and vendors. While most of the user authentication solutions may provide all the core functionalities, their breadth and depth may differ by different vendors' offerings. Driven by increasing competition, vendors are increasingly looking at improving their technology capabilities and overall value proposition to remain competitive. Some of the key differentiators include:

- **The Sophistication of Technology Platform:** Users should evaluate a user authentication solution that offers comprehensive capabilities to manage, authenticate, and secure access to employees, customers, and partners. The solution should also offer access management, MFA, single sign-on, analytics and reporting, and user directory support. However, with the rising need for cost-effective, seamless, and secured access to applications and resources hosted in hybrid environments, organizations are looking for robust, scalable, and agile solution like User Authentication. Organizations prefer vendors whose products offer easy integration with other security tools to prevent vulnerabilities, easy management, operability in multi-cloud environments, ability to identify and defend against novel security threats, support for mobile apps/infrastructure, and self-service capabilities. User Authentication vendors are focusing on providing robust authentication mechanisms like adaptive risk-based multi-factor authentication with biometric verification capabilities. Vendors are using advanced analytics techniques like identity analytics and UEBA (User and Entity Behavior Analytics) to ensure enhanced security and authenticate users in real-time. In addition, the vendor should offer an intelligent AI-driven platform to allow the users to detect blind spots, authenticate and authorize users, secure identities and organizational applications, provide end-user access to resources, and detect and respond to threats in real-time. Additionally, the vendors' customer value proposition may vary in terms of ease of deployment, ease of use, price/performance ratio, support for a broad range of use cases, global support, flexible & elastic subscription service, and others.

- **Vendors' Product Strategy and Roadmap:** The vendors' ability to formulate a comprehensive and compelling technology roadmap is a crucial factor for users while adopting a user authentication platform. As a part of their technology vision and roadmap, User Authentication vendors are planning to develop innovative solutions by combining biometrics, behavior, locations or proximities, signal detecting capabilities, and utilizing integrated machine learning (ML) and artificial intelligence (AI) engines. The vendor should have

a firm understanding of the market dynamics to analyze the potential investments of their assets. To gain a competitive edge or become a pioneer in the security industry, the vendor should have strong strategic objectives and the ability to identify the trends that can be implemented across their business. Users should evaluate vendors that are well-versed with the upcoming opportunities in the user authentication market and have the ability to devise compelling strategies to overcome unprecedented events. The roadmap may include upgrading existing technology, implementing modern AI/ML-driven technologies, product launch, and more. Users should consider the vendor's focus on potential investments in mergers and acquisitions and partnerships, as well as R&D of new platform features and functionalities. Users should also evaluate the vendor's ability to leverage capabilities of AI/ML, analytics, transformation, and automation across their business and applications. It is also critical for users to evaluate vendors with the necessary expertise to execute the outlined roadmap. In addition, users need to assess the vendor's ability to set benchmarks and deadlines for their strategy and roadmap.

- **Integration and Interoperability:** Users should look for vendors of user authentication solutions that offer extensibility and support integration with existing security policies and tools. Users should look for vendors that offer extensibility and support integration with existing security policies and tools. They should also support broad integration capabilities to provide passwordless authentication for any application or service, including Windows desktops (physical or virtual), SaaS & web applications, networking & VPN, and legacy applications. Additionally, they should also support out-of-the-box integration with Citrix Workspaces, AWS, Google Cloud, IAM solutions like Microsoft, Okta, Ping Identity, ForgeRock, VPN offerings, and direct application integration via APIs. The vendor should offer off-the-shelf, UEBA, standards-based solutions integrations, self-service IAM application integration capabilities, OOTB integration with Microsoft O365, integrations with different risk, fraud, and threat signals for better authentication decisions.

- **Vendor's Expertise and Domain Knowledge:** Organizations should evaluate the vendors' expertise and domain knowledge in understanding their unique business problems, use cases, and industry-specific requirements. Organizations are advised to conduct a comprehensive evaluation of different user authentication solutions and vendors before making a purchasing decision. Requirements of user authentication features may differ significantly for various users from SMBs to large enterprise organizations. Users should employ a weighted analysis of the several factors important to their specific organization's use cases and industry-specific requirements. Users should also look for a user authentication solution with a history of successful large-

scale deployments and carefully analyze the existing case studies of those deployments. This should form the basis to prepare best-practice user authentication solution deployment.

- **Scalability:** A user authentication vendor should offer a sophisticated solution that can authenticate users in real-time and secure privileged organizational resources and applications. The vendor of a user authentication solution should offer a sophisticated solution that can authenticate users in real-time and secure privileged organizational resources and applications. The solution should be able to support a liberating mobile onboarding experience, seamless and secure user access, including passwordless with mobile push authentication, frictionless portal access, transaction verification, and help facilitate regulatory compliance. The User Authentication vendor should provide a cross-platform-supported authentication solution to meet enterprise-class security requirements to ensure that organizations can leverage the solution for both internal and external user communities. Also, the solution should be able to handle millions of user identities at individual customers and hundreds of millions of devices identities at individual customers. Many user authentication vendors are increasingly supporting an unrivaled number of authenticators, including OTP, hard tokens, FIDO2, soft tokens, mobile push notifications, grid cards, voice OTP, biometrics, smart cards, PKI Certificates, OATH Compliant tokens, and mobile SDK, for custom applications. Additionally, user authentication should support digital onboarding, and facial, voice, fingerprints, and behavioral authentication, on both mobile and web channels. However, the depth of technical functionalities and capabilities for authorization of different users may differ from vendor to vendor.

- **Zero Trust Security:** Zero trust security helps organizations secure their organizational assets against data breaches and modern cyber-attacks by verifying insiders or outsiders through a network perimeter. It helps secure user access to applications and information irrespective of the location, time, and nature of the device used by authenticating and authorizing users in real-time. Currently, organizations are actively participating in the CAEP/SSE OpenID standards project to increase their risk management capabilities and zero trust competitiveness. Zero trust security helps minimize cyber threats by allowing organizations to provide access to only those authorized to access the resources.

- **Maturity of AI and ML technology:** User authentication vendors' capability to provide embedded AI and machine learning capabilities may differ significantly. AI/ML is maturing across the security industry and helping organizations identify, authenticate, and authorize users connected to the network resources in real-time. Organizations can leverage AI and ML to

automatically and continuously authenticate users to enhance security. Users should look at vendors offering AI/ML for authorizing user access, enhancing efficiency, restricting access of bad actors and bots, and automating API discovery.

- **Robust Security**: User authentication vendors are providing robust security by securing cloud and network in real-time. Features offered by vendors differ significantly for different users, from SMBs to large enterprise organizations. Some of the user authentication vendors are actively participating in the CAEP/SSE OpenID standards initiative to strengthen their risk management capabilities and zero trust competitiveness. Additionally, users should look for user authentication vendors who can help to improve the network, user authorization, application, and data security, reduce fraud, and address specific threats and regulatory requirements.

SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's competitive landscape analysis is a useful planning guide for strategic decision makings, such as finding M&A prospects, partnership, geographical expansion, portfolio expansion, and others.

Each market participant is analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make SPARK Matrix.

Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%

Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

Evaluation Criteria: Technology Excellence

- **The sophistication of Technology**: The ability to provide comprehensive functional capabilities and product features, technology innovations, product/platform architecture, and such others
- **Competitive Differentiation Strategy**: The ability to differentiate from competitors through functional capabilities and/or innovations and/or GTM strategy, customer value proposition, and such others.
- **Application Diversity**: The ability to demonstrate product deployment for a range of industry verticals and/or multiple use cases.

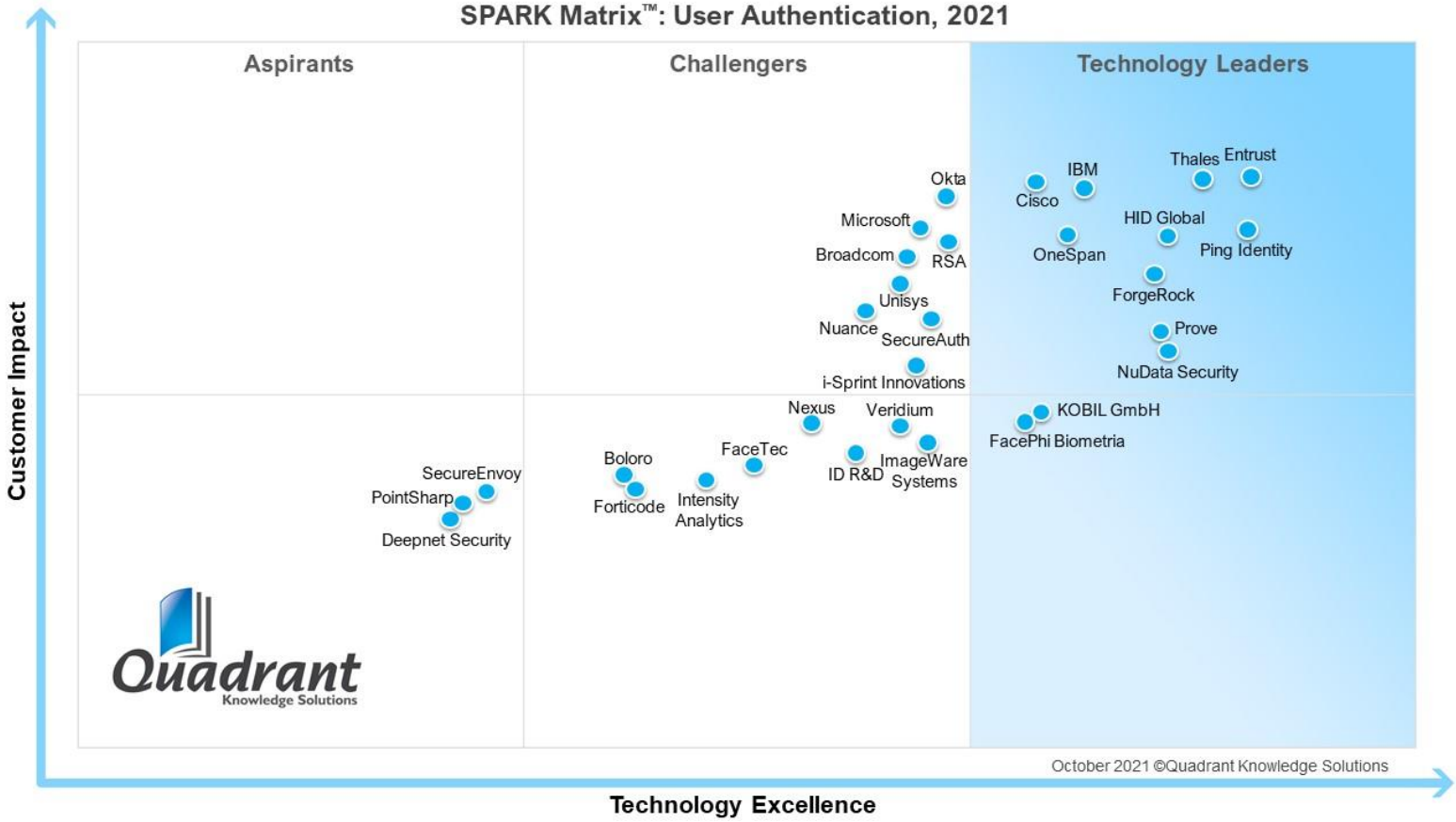
- **Scalability**: The ability to demonstrate that the solution supports enterprise-grade scalability along with customer case examples.
- **Integration & Interoperability**: The ability to offer product and technology platforms supporting integration with multiple best-of-breed technologies, providing out-of-the-box integrations, and open API support and services.
- **Vision & Roadmap**: Evaluation of the vendor's product strategy and roadmap with the analysis of key planned enhancements to offer superior products/technology and improve the customer ownership experience.

Evaluation Criteria: Customer Impact

- **Product Strategy & Performance**: Evaluation of multiple aspects of product strategy and performance in terms of product availability, price to performance ratio, excellence in GTM strategy, and other product-specific parameters.
- **Market Presence**: The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.
- **Proven Record**: Evaluation of the existing client base from SMB, mid-market and large enterprise segment, growth rate, and analysis of the customer case studies.
- **Ease of Deployment & Use**: The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation, and usage experience. Additionally, vendors' products are analyzed to offer a user-friendly UI and ownership experience.
- **Customer Service Excellence**: The ability to demonstrate vendors capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.
- **Unique Value Proposition**: The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

SPARK Matrix™: User Authentication
Strategic Performance Assessment and Ranking

Figure: 2021 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
User Authentication Market



Vendor Profiles

Following are the profiles of the User Authentication vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process, along with publicly available information. The Quadrant research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technical capabilities. Users are advised to consult Quadrant Knowledge Solutions before making any purchase decisions regarding User Authentication technology and vendor selection based on research findings included in this research service.

Cisco

URL: http://www.cisco.com

Founded in 1984 and headquartered in San Jose, CA, US, Cisco is a leading provider of networking solutions, communications and collaboration solutions, security and a variety of other technology services and products. Cisco provides user authentication through its user-friendly access security platform Duo. The platform offers secured access to all applications and resources through its comprehensive capabilities, including multi-factor authentication (MFA), device trust, adaptive access policies, remote access, and single sign-on (SSO) to protect organizations from unauthorized access, data breaches, and security threats.

Cisco Duo's MFA capability allows organizations to secure all applications on any device by verifying user identities before providing access. Additionally, the capability includes an administrative dashboard, detailed reporting, and an up-to-date cloud-based model to prevent threats in real-time. Cisco Duo Device Trust enables organizations to identify risky devices, implement contextual access controls across managed and unmanaged devices, and report on device health by leveraging an agentless approach or integrating with the user's device management system. Cisco Duo Device Trust provides reporting capabilities and an admin-friendly dashboard to easily monitor security policies and detect unusual login behavior. Additionally, Duo Device Health and Self-Remediation and Duo Mobile App's Security Check-up allow the user to take responsibility for their laptop and mobile device health. Cisco Due Device Trust also prevents out-of-date devices from accessing the company services by providing automated reminders about software update reminders.

Cisco's Duo Adaptive Access Policies allow organizations to create customized access controls depending on role, device, location, and other contextual aspects. Cisco's Duo Adaptive Access Policies enables organizations to secure applications and data from compromised or risky devices in real-time by enforcing security policies for all devices. Additionally, it allows admins to configure rights based on the operating system and particular device settings and automatically informs users when their software is out of date. Cisco's Duo Adaptive Access includes application-specific control to easily onboard contract employees, adjust access permissions, and protect high-value data with tight security policies.

Cisco's Duo Remote Access provides secured access to applications and servers by authenticating identity and device trust regardless of how, where, or when users log in. It allows organizations to protect on-prem and cloud environments such as Microsoft Azure, Amazon Web Services, and Google Cloud Platform, with or without VPN. Cisco's Duo Remote Access offers a new remote access solution or allows organizations to add an extra layer of security to existing VPNs with multiple integrations, including Cisco AnyConnect, Juniper, Citrix, F5, and others. Additionally, it allows organizations to easily set per app access policies and provides secured SSH access.

Cisco's Duo SSO offers secured access to any application, regardless of its deployment model, from a single dashboard. Additionally, it allows admins to customize access policies per application, including granular access policies that provide the right level of access to the user, and supports existing SSO, federation, and identity providers. Cisco Duo enables organizations to secure application access based on organizational needs by integrating the zero-trust platform with other SSO and identity provider solutions.

Analyst Perspective

Followings are the analysis of Cisco's capabilities in the global User Authentication market:

- Cisco offers a cloud-based, flexible, user-friendly, super-secure user authentication solution through its platform Duo. The solution allows organizations to authenticate user identities, gain insight into every device, and implement adaptive controls to secure access to the network, resources, and privileged data. Cisco Duo allows organizations to add Duo to any existing environment or platform. Additionally, it offers a self-enrollment feature for easy deployment.

- Concerning geographical presence, Cisco has a strong presence in the USA. From the industry vertical perspective, the company has a presence across a wide variety of industry verticals, including healthcare, manufacturing, electric utilities, energy, education, financial services, government, retail, sports and entertainment, and transportation. From a use case perspective, Cisco supports cloud apps, VPNs, firewalls, desktop protection, passwordless authentication, zero-trust security, workforce authentication, website/user authentication, and phishing prevention.

- Cisco's primary challenges include the growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value proposition, Cisco is well-positioned to maintain and grow its market share in the User Authentication market.

- Concerning technology roadmap, Cisco is focusing on enhancing user authentication capabilities, passwordless authentication, increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

Entrust

URL: https://www.entrust.com

Founded in 1969 and headquartered in Shakopee, MN, US, Entrust is a well-known identity and access management (IAM) provider enabling trusted identities for workforces, consumers and citizens. The company offers best-in-class identity proofing, multi-factor authentication (MFA), single sign-on (SSO), access control, and adaptive risk-based authentication that is easy to deploy and manage. Entrust's unified IAM portfolio enables a Zero Trust approach that helps protect against unauthorized access, data breaches and other cyberattacks, and fraudulent transactions.

Entrust IAM supports consumers with a liberating mobile onboarding experience, seamless secure user access including passwordless with mobile push authentication, frictionless portal access, transaction verification, and helps facilitate regulatory compliance. Fraud detection and prevention is made possible with behavioral biometrics and analytics. As well, Entrust IAM supports the seamless secure delivery of government services to citizens including e-passports / digital travel credentials (DTC), digital national IDs, and mobile driver licensing.

From a workforce perspective, Entrust IAM provides secure employee access to cloud and on-premises applications both in the office and remotely via VPN. Secure device provisioning via enterprise mobility management (EMM) integrations help protect worker devices and communications with encryption and signing. Entrust keeps worker friction to a minimum with passwordless login, SSO and adaptive risk-based authentication. As well, Entrust IAM offers high assurance workforce solutions including PKI-based credentials and Personal Identity Verification (PIV) compliance for U.S. government workers.

Entrust IAM unburdens IT with user self-service tools including password resets, off-the-shelf integrations, a flexible risk-based policy engine, role-based access control (RBAC) and developer APIs and SDKs. As well, Entrust IAM seamlessly integrates with an organization's existing IT infrastructure including directories such as Microsoft AD, Azure AD and/or other LDAP sources. Identity orchestration helps IT teams seamlessly navigate hybrid / multi-cloud environments with SAML and OIDC. As well, superior URL/API protection is provided using OAuth 2.0/2.1.

Entrust IAM provides support for an unrivalled number of authenticators including OTP, hard tokens, FIDO2, soft tokens, mobile push notifications, grid cards, voice OTP, biometrics, smart cards, PKI Certificates, OATH Compliant tokens, and mobile SDK for custom applications. Entrust supports different deployment options, including cloud (SaaS), on-premises, hybrid, or as a virtual appliance. Additionally, Entrust IAM is available as a managed service from one of the company's MSP partners.

Analyst Perspective

Followings are the analysis of Entrust's capabilities in the global User Authentication market:

- Entrust provides a cloud-based, holistic identity and access management (IAM) solution to protect financial transactions, manage citizen IDs, and protect digital businesses through authentication, digital certificates, and secured communication. Entrust IAM utilizes high-assurance credential-based access, single sign-on (SSO), passwordless access, best-in-class multi-factor authentication (MFA), adaptive risk-based access and authentication, identity proofing, and secure portals to protect identities, payments, access, privileged data.

- Some of the key differentiators of the Entrust IAM include high assurance credential-based access management, self-service for all users, including password reset, account unlocking, and policy-based authentication management, adaptive risk-based authentication policy engine with self-learning capabilities and multi-tier functionally, a broad range of authentication techniques with self-service support, and out-of-the-box integration with fraud detection, ID proofing, 3DS, and RASP to secure compliance with standards like as PSD2, GDPR, and others.

- Concerning geographical presence, Entrust has a strong presence in the USA and Canada, followed by Europe, Middle East & Africa, Asia Pacific, and Latin America. From the industry vertical perspective, the company has a presence across a wide variety of industry verticals, including healthcare & life sciences, energy & utilities, manufacturing, IT & telecom, banking & financial services, education, retail & eCommerce, and govt & public sectors. From a use case perspective, Entrust supports cloud apps, VPNs/ firewalls, desktop protection, credentials-based passwordless access, Linux PAM, and ADFS / ISAPI/ Apache Filter.

- The primary challenges before Entrust include the growing competition from emerging vendors with innovative technology offerings. These vendors have successfully gained a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its sophisticated technology platform, comprehensive functional capabilities, robust roadmap, compelling customer references, and customer value proposition, Entrust, is well-positioned to maintain and grow its market share in the User Authentication and Authorization market.

- Concerning technology roadmap, Entrust is investing in Identity and Access Management solutions with UEBA integrations and IGA capabilities. Additionally, the company is focusing on increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

FacePhi Biometría

URL: https://www.facephi.com

Founded in 2012 and headquartered in Alicante, Comunidad Valenciana, Spain, FacePhi is a leading Spanish company in the field of technology for users' digital identity verification, specializing in digital onboarding and biometric authentication solutions, with +39 million users. As global leaders in the banking sector, FacePhi offers cutting-edge technology that protects, in a consensual way, the digital identity of customers in all their interactions.

FacePhi authentication solutions provide account access or transactions approval with biometrics. FacePhi leverages access and transactions to prevent phishing, spoofing, and Man-in-the-Middle attacks. It also provides a light and intelligent learning pattern, an encrypted and tokenized pattern, picture, and video detector, and does not send images to the bank while accessing an account or any operation.

FacePhi digital onboarding solution provides a secure onboarding with real-time OCR and facial passive liveness tests. It allows users to open an account or access any product from any location by taking a selfie and capturing the ID document. Additionally, it includes fast OCR process and facial verification, pattern sending no image, lightweight encrypted and tokenized patterns, picture and video detector, validation of DNI's at fraud level, Passive Liveness as Proof of Life, and supports all types of documents with MRZ or PDF416-417, QR and barcodes.

Analyst Perspective

Followings are the analysis of FacePhi's capabilities in the global User Authentication market:

- FacePhi offers a comprehensive and customized solution for digital onboarding, authentication, and security by leveraging different biometric and anti-fraud technologies. The FacePhi solution includes multifactor biometrics, transaction dashboard, multiplatform solution, provides 24/7 support, and helps users minimize integration time. Some of the key differentiators of FacePhi include on-premise installation, multimodal installation, automatic capture and real-time OCR, certified passive liveness, and tailor-made solutions.

- From a geographical presence perspective, FacePhi has a strong presence in Latin America and Europe, followed by the Asia Pacific and the Middle East & Africa. From an industry vertical perspective, the company holds a customer base across various sectors, including banking & financial services, govt & public sectors, healthcare, insurance, traveling & transportation and more. From a use case perspective, FacePhi supports digital onboarding, as well as facial, voice, fingerprints and behavioural authentication, on both mobile and web. Both the

onboarding processes and subsequent authentications have numerous security features, such as document validation, connection to government databases, and blacklists corroboration.

- The primary challenges for FacePhi include the competition from well-established vendors with innovative technology offerings. Additionally, the company might face some challenges in expanding its presence across the USA and Canada markets due to the presence of other players with higher brand visibility. However, with its comprehensive functional capabilities, compelling technology differentiation, and robust customer value proposition, FacePhi is well-positioned to maintain and grow its market share in the digital identity market.

- As part of its technology roadmap, FacePhi is investing in a comprehensive digital identity verification platform with real-time onboarding and authentication flows, transaction control, and results statistics. Additionally, the company is focusing on increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

ForgeRock

URL: https://www.forgerock.com

Founded in 2010 and headquartered in San Francisco, California, USA, ForgeRock is one of the leading players in the user authentication market. ForgeRock offers comprehensive identity and access management solutions to provide secure access for an organization's customers as well as employees. ForgeRock enables organizations to orchestrate, manage, and protect the lifecycle of identities through dynamic access controls, governance, APIs, and storing authoritative data in any cloud or hybrid environment. Additionally, ForgeRock provides secured access to privileged data and blocks unauthorized users in real time.

ForgeRock offers a comprehensive suite to provide user authentication features. ForgeRock offers 'Adaptive Risk' which is a part of its intelligent access platform and has absolute control in granting access to the resources. The solution considers several factors like device type, IP address, operating system (OS), browser, time of the day, network type, etc. The feature helps verify the user's identity and analyzes the device type and the location once the user logs in, after which the user is provided with either an OTP or a push notification to make authentication for users fast and simple. It also helps minimize data breaches and the level of risk and suggests required actions whenever an anomaly is detected. ForgeRock's adaptive risk engine detects and responds to suspicious activity and anomalies, and monitors suspicious users. ForgeRock further enhances the authorization process in real-time and enables companies to compare contextual data consistently.

ForgeRock utilizes numerous Multi Factor Authentication (MFA) options and intelligent risk engines. It also offers passwordless authentication to enhance the user experience. ForgeRock offers the adaptive risk capability which demands an extra authentication process if the risk level is detected high and eases the process of authentication when the risk is low, which minimizes friction and provides a seamless user experience. The company's intelligent authentication capability enables organizations to integrate with cybersecurity solutions, use existing authenticating options, and create custom authenticators based on their requirements. The company also provides self-service tools for forgotten passwords, registration, and updating profiles.

Analyst Perspective

Following is the analysis of ForgeRock's capabilities in the User Authentication market:

- ForgeRock's intelligent identity platform offers a robust suite of solutions for user authentication which helps organizations to secure the identity of users and devices in real-time. ForgeRocks's Adaptive Risk capability helps protect the organization with minimum friction with passwordless authentication. Furthermore, the company offers authentication methods such as behavioral biometrics and favours all types of user senarios. ForgeRock also supports identity types like workforce/employees, and consumers.

- ForgeRock offers automated and secure onboarding and delivers a secure ecosystem (devices, services, and users). It also offers lifecycle management, zero-touch authentication, authentication of attached sensors and services, fine-grained device authorization, and relationship management between user and device. The company also offers continuous authorization with single sign on (SSO) to provide access to all the applications for all users.

- In terms of geographical presence, ForgeRock has a strong global presence with offices at major locations in the USA, Europe, and the APAC region. ForgeRock has a presence in many industry verticals, including financial services, telco & media, retail, auto & smart mobility, government, healthcare, education, energy, engineering, and insurance. From a use case perspective, ForgeRock offers passwordless authentication, contextual authorization, single sign-on, lifecycle management, API security, legacy integration, and more.

- ForgeRock's key challenges include the growing competition from emerging vendors with innovative technology offerings who tend to serve a certain section of employees. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-sized organizations and are amongst the key targets for mergers and acquisitions. However, with its comprehensive functional capabilities, compelling customer references, and robust customer value proposition, ForgeRock is well-positioned to maintain and grow its market share.

- Concerning technology roadmap, ForgeRock is investing on increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

HID Global

URL: https://www.hidglobal.com

Founded in 1991 and headquartered in Austin, Texas, US, HID Global is a well-funded company with a proven track record of delivering identity & access management (IAM) solutions to the world's leading companies and governments. Around 90% of Fortune 500 companies use HID solutions today to power the trusted identities of the world's people, places and things. HID Global allows organizations to detect, verify, and authenticate users through its HID Global Authentication Platform, encompassing solutions, such as Authentication Service, WorkforceID Authentication, HID Approve™, WorkforceID Digital Credential Manager, Crescendo® Smart Cards and Security Keys, Risk Management Solution and Identity Verification Service.

HID Global offers a safe, scalable authentication platform for trusted identity and access management which allows organizations to integrate user authentication and authorizations easily and quickly into their business applications and solutions. The platform offers many alternatives available in the cloud or on premise.

The cloud based HID Authentication Service and WorkforceID™ Authentication enable consumer and workforce authentication. Both solutions are equipped and compatible with a wide array of authenticators, one of which being HID Approve™. HID Approve™ allows to authenticate access requests and sign transactions either on a mobile device or PC using multi-factor authentication to meet identity privacy and data protection compliance requirements. Additionally, HID Approve™ can provide a secure code or push notification.

HID Global also offers cloud-based management of workforce authenticators via WorkforceID™ Digital Credential Manager, which enables organizations to centrally issue and manage high assurance credentials and PKI-certificates in a multi-tenant cloud environment managed by Amazon AWS. WorkforceID™ Digital Credential Manager allows organizations to implement a zero-trust model by empowering them to deploy strong public key-based two-factor authentication, manage and monitor secure physical access to buildings and digital access to networks and cloud applications from a single platform, integrate with open standard protocols and Active Directory Federation Services (ADFS) by utilizing SAML. Additionally, the solution supports a diverse range of authentication methods and form factors to provide various security level options. It also supports FIDO2 PIN Management to streamline enterprise deployment of FIDO2 and WebAuthn with HID Crescendo® authenticators.

HID Crescendo® authenticators provide organizations with high-assurance digital credentials by leveraging certified cryptography in compliance with NIST authenticator assurance level SP800-63 IAL2/IAL3. HID Crescendo® authenticators allow organizations to secure corporate networks, data and applications while meeting legal obligations. Use cases include secure PC and network logon, remote and cloud access, privileged access, email and document signing and encryption, Crescendo® smart cards can also be used

as a corporate badge, protecting access to facilities, in addition to protecting access to digital/IT resources. HID Crescendo® authenticators leverage a variety of protocols, including FIDO2, PIV/PKI, and OATH, to enable interoperability with a wide range of applications. Additionally, HID Crescendo® smart cards are fully supported by HID Signo, iCLASS SE and multiCLASS SE reader platforms for traditional physical access. HID Crescendo® authenticators include HID Crescendo® C2300 Series, HID Crescendo® Key Series, HID Crescendo® 144K FIPS Series, HID Crescendo® PIV, and HID Crescendo® Temporary Access Card.

HID Global also offers data analytics-based real-time risk profiling technology via its HID Risk Management Solution. The solution allows financial institutions to detect and secure traditional and modern threats to prevent fraud targeting online and mobile banking channels. The solution utilizes artificial intelligence (AI) and machine learning-based algorithms to offer detection capabilities through three detection engines that constantly analyze and detect behaviors anomalies and threats. Additionally, when integrated with the HID Authentication Platform, it provides adaptive or risk-based authentication to secure user IDs, transactions, devices, and accounts.

HID Global also offers a customizable onboarding solution titled Identity Verification Service. The solution allows organizations to securely create customer digital onboarding journeys with up to 70 technical checks and 50-point facial biometric comparison. HID Identity Verification Solution provides a frictionless user experience to minimize customer abandonment rates. It also provides pre-built architecture and cloud-based distribution for fast deployment, improved integration, an all-inclusive pricing model for a low total cost of ownership (TCO), built-in compliance with eKYC regulations from government agencies, and AI-powered technology and trustworthy database validation for greater assurance and better matching. The combination of the Identity Verification Service, Risk Management Solution and the Authentication Platform offers a seamless end-to-end customer banking journey.

Analyst Perspective

Followings are the analysis of HID Global's capabilities in the global User Authentication market:

- HID Global offers robust, out-of-the-box solutions to authenticate the users in real-time and protect organizations from various threats. HID Global offers a wide variety of authenticators and form factors, including multi-protocol (FIDO, PKI/PIV, OATH) smart cards and security keys, mobile and hardware one-time password (OTP) tokens, and physical access cards to authenticate users at workstations or federated websites/applications. HID Global supports multiple authentication methods, including username and password, OTP, Biometrics, push-based mobile authentication using asymmetric keys, behavioral analytics, risk-based authentication, out-of-band authentication and others.

- HID Global allows organizations to protect users, websites, and IoT devices. Some of the key differentiators of HID Global are leader in identity and access management technology, trusted by governments, financial institutions, and provides easy deployment and integration with standards-based solutions. Additionally, the HID Authentication platform includes the award-winning HID Approve™ solution, which combines asymmetric key-based cryptography with push notifications (available as SDK).

- From a geographical presence perspective, HID Global has a strong presence in Europe and the US, followed by Middle East & Africa, Asia Pacific, and Latin America. From an industry vertical perspective, the company holds a customer base across various sectors, including govt & public sectors, healthcare & life sciences, travel & hospitality, IT & Telecom, energy & utilities, and manufacturing. From a use case perspective, HID Global supports consumer authentication for retail banking, user authentication in corporate banking, authentication of doctors prescribing controlled substances (EPCS), workforce authentication, and website/user authentication.

- The primary challenges of HID Global include growing competition from emerging vendors with innovative technology offerings as well as continued competition from well-established vendors. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its strong domain experience, global footprint and integrated technology strategy, HID Global is well-positioned to maintain and grow its market share, especially in the large enterprise and mid-market customer segments.

- As part of its technology roadmap, HID Global is focusing on cloud-first approach/cloud-native containerization supporting both on-premises and customer-managed cloud, improve mobile security. The company also plans to expand its biometrics portfolio and its business process orchestration capabilities. The company is also expanding its portfolio via acquisition or investment. Additionally, HID IAMS continues to embrace industry standards like FIDO and to enable more FIDO-based credentials.

IBM

URL: https://www.ibm.com

Founded in 1911 and headquartered in Armonk, New York, IBM is a leading provider of IT technology, cloud platforms, and consultancy services. The company offers computer hardware, software, infrastructure, and hosting services. IBM offers robust users authentication capability as an integral part of its security and identity portfolio. IBM enables organizations to secure privileged data and access by identifying and authenticating users in real-time.

IBM allows organizations to authenticate users via its QRadar User Behavior Analytics, which provides visibility into behavioral anomalies, allows organizations to analyze user activity to identify malicious insiders, and verifies users' credentials to determine whether they are hacked or not. Additionally, IBM QRadar User Behavior Analytics allows organizations to identify risky users, analyze unusual behavior, and minimize users' risk scores by examining underlying log and flow data. IBM also provides authentication modules that trigger specific challenges and authentication technology to authenticate the user by either the username and password or a one-time password.

IBM enables administrators to identify and control information included in the credentials, utilize the credential editor to set the properties to be included in creating credentials, and use authenticationTypes and authenticationMechanismTypes features to author an access control policy to authenticate users and secure the organizational data in real-time. IBM authenticates user identity and provides authorized user access with its comprehensive authentication mechanisms, including one-time password authentication, MAC one-time password authentication, HOTP one-time password authentication, TOTP one-time password authentication, RSA one-time password authentication, username and password, HTTP redirect, consent to device registration, and FIDO universal second factor.

IBM allows organizations to use simple authentication, step-up authentication, and multi-factor authentication by integrating different authentication methods into the authentication policy workflow. Additionally, IBM provides web-based authentication using HTML template files and responses and REST API-based authentication using JSON template files and responses. IBM allows organizations to use configuration scenarios to build custom configuration, configure HOTP one-time password mechanism, TOTP one-time password mechanism, MAC one-time password mechanism, RSA one-time password mechanism, one-time password delivery methods, username and password authentication, HTTP redirect authentication mechanism, consent to device registration, end-user license agreement authentication mechanism, email message mechanism, reCAPTCHA verification authentication mechanism, info map authentication mechanism, knowledge questions authentication mechanism, FIDO universal second-factor authentication mechanism, QR code authentication mechanism, authentication and

access module for cookieless operation, enable or disable authentication policies, and manage mapping rules.

Analyst Perspective

Followings is the analysis of IBM's capabilities in the global User Authentication market:

- IBM offers comprehensive user authentication solution to identify, authenticate, and authorize users connected to the network resources in real-time. IBM leverages various technologies, including SSL client certificates, SSH keys, user IDs and passwords, client IP addresses, and RSA SecurID to authenticate and authorize users. Additionally, the company enables application outputs, which allow users to map attributes returned by a query, such as login credentials, to user-defined outputs. IBM supports system authentication, RADIUS authentication, TACACS authentication, Microsoft Active Directory, LDAP, and SAML single sign-on authentication.

- Concerning geographical presence, IBM has a strong presence in the USA followed by the EMEA and the APAC region. From the industry vertical perspective, the top verticals for IBM include aerospace and defense, financial services, education, electronics, energy and utilities, healthcare, life sciences, manufacturing, media and entertainment, retail, and government & public sectors. From a use case perspective, IBM supports cloud apps, desktop protection, passwordless authentication, workforce authentication, website/user authentication, and phishing prevention.

- The primary challenges of IBM include growing competition from emerging vendors with innovative technology offerings as well as continued competition from well-established vendors. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. Additionally, the company may face challenges in improving market penetration in the key markets of the APAC region. However, with strong domain experience and integrated technology strategy, IBM is well-positioned to maintain and improve its market share, especially in the large enterprise and mid-market customer segments.

- Concerning technology roadmap, IBM is focusing on improving user authentication capabilities, increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

KOBIL GmbH

URL: https://www.kobil.com

Founded in 1986 and headquartered in Worms, Germany, KOBIL GmbH is a provider of digital and highly secure data technology. KOBIL GmbH designs, develops, and releases pre-packaged, multichannel, multiplatform identity management and mobile security software. KOBIL GmbH allows organizations to authenticate users with its products titled mIDLogin and mIDVerify. These products allow organizations to authenticate users, authorize transactions, enhance user experience, minimize fraud, and meet regulatory requirements.

KOBIL GmbH mIDLogin provides secured and trusted passwordless access to enhance user experience. KOBIL GmbH mIDLogin leverages its end-to-end encryption channel titled Digitanium to secure all logins, automatically mitigate phishing threats, detect instances of theft, app manipulation, user impersonation and man-in-the-middle attacks. KOBIL GmbH mIDLogin continuously authenticates digital identities and provides access only to the approved resources. Additionally, it helps organizations secure access, apps, devices, privileged data, and business workflows by identifying, authenticating, and authoring users connected to the network resources in real-time.

KOBIL GmbH mIDVerify authenticates and provides the right level of access to the right users to the right app or network resources for every login or transaction in real-time. KOBIL GmbH mIDVerify allows organizations to accept or decline transactions with one click, provides unprecedented access, whether online or offline, and supports fingerprint and face recognition to provide flexible access to all types of users and operating systems. Additionally, KOBIL GmbH provides virtual smart card technology and world-leading PKI technology for user authentication, authorization, and PKI-based digital signatures. KOBIL GmbH also offers a Smart Security Management Server (SSMS) to manage end-to-end encrypted communication in real-time between application companies. Additionally, the company’s solutions comply with all industry regulations and support iOS, Android, Android, iPadOS, macOS, and Windows or IoT devices for the identification of users.

Analyst Perspective

Followings is the analysis of KOBIL GmbH's capabilities in the global User Authentication market:

- KOBIL GmbH offers a robust user authentication solution through its mIDLogin and mIDVerify products to authenticate and authorize users in real-time. KOBIL GmbH mIDLogin and mIDVerify consist of secured features, including application shielding, real-time security servers, Digitanium channel, PKI-based virtual smart card technology (public-key credentials for smartphones), the binding identity of app, device, and person, support for multiple users per device, and one user using multiple devices. KOBIL GmbH mIDLogin leverages different login methods such as Face ID, Fingerprint, QR-Code, PIN, OTP apps for smartphones, OOBS SMS to authenticate user in real time.

- Concerning geographical presence, KOBIL GmbH has a strong presence in Europe and the Middle East. From the industry vertical perspective, the top verticals for KOBIL GmbH include banking & financial services, IT & telecom, education, insurance, and such others.

- The primary challenges for KOBIL GmbH include the competition from well-established vendors with innovative technology offerings. Additionally, the company might face some challenges in expanding its presence across the USA and Canada markets due to the presence of other players with higher brand visibility. However, with its comprehensive functional capabilities, compelling technology differentiation, and robust customer value proposition, KOBIL GmbH is well-positioned to maintain and grow its share in the digital identity market.

- Concerning technology roadmap, KOBIL GmbH is focusing on improving user authentication capabilities, increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

NuData Security, a Mastercard Company

URL: https://nudatasecurity.com

NuData Security is a Mastercard company. Founded in 2008 and headquartered in Vancouver, British Columbia, NuData helps businesses verify good users without disruption and stop bad actors before they can cause damage. By assessing over 1.7 billion behavioral events each month, NuData harnesses the power of behavioral biometrics and device intelligence to verify users, stop account takeover, prevent new account fraud, and reduce good user friction in real time.

NuData has three levels of customizable solutions:

NuDetect for Continuous Validation enables organizations to authenticate good user behavior to provide a secure and frictionless experience, from login to logout. NuDetect for Continuous Validation allows organizations to continuously detect unusual behavior of users with machine learning, protects users by analyzing user behavioral data and device-based information, and customize security rules to meet business needs. NuDetect for Continuous Validation monitors all the activity across the session, blocks high-risk traffic in real-time, identifies good and bad users, and minimizes risk with enterprise-grade security control.

NuDetect for Good User Validation provides secured account access to good users, enhances the user experience, evaluates hundreds of anonymized user data points as they interact with the organizational environment, and identifies trusted users even the online habits changes with the help of machine learning. Additionally, it provides users risk scores to detect good customers and allows organizations to block high-risk traffic in real-time and prevent future fraud.

NuData offers a bot detection solution, NuDetect for Account Takeover, to prevent automated attacks like account takeover. NuDetect for Account Takeover prevents attacks before they access the organizational login interface, allows organizations to customize the solution, and utilizes behavioral analytics technology combined with its Trust Consortium to detect automated threats in real time. Additionally, the solution helps by providing trust scores to minimize risk and friction, detects good customers, and reduces manual reviews.

NuData Security allows organizations to deploy NuDetect for Continuous Validation and NuDetect for Good User Validation anywhere using AWS, Azure, GCP, or even in their own data center. NuDetect for Continuous Validation and NuDetect for Good User Validation supports different operating systems, including iOS, Android, Windows, tablet, or mobiles. Additionally, the company provides daily traffic reports when high-volume attacks are observed.

Analyst Perspective

Followings are the analysis of NuData Security's capabilities in the global User Authentication market:

- NuData Security offers behavioral analytics and passive biometric-based NuDetect to detect digital users in real time. NuDetect analyzes millions of devices, locations, passive biometric and behavioral signals with previous user behavior and known patterns to authenticate users. Additionally, NuDetect integrates multi-layered technology to allow organizations to identify valid users and fraud risks in real-time, improve the user experience, and identify unknown users. NuDetect provides continuous and accurate validation of user behavior in real time. It also provides intelligent automation detection and allows the identification of threats during the application/registration process to make confident judgments.

- NuData Security's NuDetect provides a good user experience, multi-channel security and mitigates human-driven attacks. It provides customized security, accurate real-time scores for best-in-class behavioral validation, real-time detection and analysis tools to identify and prevent fraud. NuDetect offers aggregated behavioral intelligence by utilizing machine learning techniques and billions of behavioral data points for accuracy. It also provides continuous real-time fraud detection and user verification as well as award-winning technology to verify users and provide a great customer experience. Additionally, it enables analysts to conduct in-depth forensic investigations of events and detect fraud and cyber-attacks in the case of an increase in automated online attacks.

- Concerning geographical presence, NuData Security has a strong presence in Canada and the US. From an industry vertical perspective, the company holds a customer base across various sectors, including banking and financial, eCommerce, digital goods, and government. From a use case perspective, NuData Security supports automated attacks, fighting account takeovers, user recognition, card testing, new account fraud, and loyalty fraud.

- NuData Security's primary challenges include the growing competition from emerging vendors with innovative technology offerings as well as from small vendors focusing on local geography who tend to serve a certain section of employees. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with comprehensive functional capabilities, compelling customer references, and a robust customer value proposition, NuData Security is well-positioned to maintain and grow its market share.

- As part of its technology roadmap, NuData Security is focusing on improving behavior signals within its rules engine, integrating with Mastercard Identity

Check, expanding connected intelligence across Mastercard network, and enhancing its behavioral biometrics capabilities. Additionally, the company is focusing on increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

OneSpan

URL: https://www.onespan.com

Founded in 1991 and headquartered in Chicago, Illinois, USA, OneSpan provides secure digital identity and anti-fraud solutions. OneSpan provides risk-based adaptive authentication, digital identity verification, and next-generation solutions through its cloud-based platform. The OneSpan Trusted Identity Platform makes it easy to integrate with new and existing tools and technologies, helps detect fraud, and improves user experience.

The Trusted Identity Platform offers a fully integrated cloud-based platform which offers identity verification, authentication, fraud prevention solutions, and e-signature, and enables organizations to deploy identity verification from a single platform. The platform's architecture can integrate with third-party technologies and meet the requirements of global compliance regulations, including SOC2, GDPR, PSD2, and ISO. The platform leverages pre-configured machine learning models for fraud prevention. Additionally, the platform leverages an advanced single orchestration layer to manage users, workflows, and integrations.

The platform offers intelligent adaptive authentication that leverages Multi Factor Authentication (MFA), risk analytics engine, and app security to improve fraud detection and prevention. OneSpan's intelligent adaptive authentication optimizes the user experience and provides security based on unique customer requirements. This is achieved by analyzing large quantities of data to identify risk scores. These scores use intelligent workflows that trigger immediate action based on customer-defined security policies and rules.

The platform offers mobile authentication applications for Android and iOS apps to secure enterprise. It offers easy deployment since employees are simply required to download the app and follow a self-service provisioning process. It offers two-factor authentication to restrict unauthorized access, improve remote access security, and protect against data breaches. The platform also offers OneSpan cloud authentication with cloud-based multifactor authentication solutions which are easy to deploy, scalable, and more flexible as compared to on-premise deployment options.

The platform offers FIDO authentication which eliminates the need for passwords with FIDO U2F, FIDO UAF, and FIDO2 solutions. FIDO authentications deploy passwordless authentication to simplify customer experience, strengthen authentication with FIDO public cryptography-plus, eliminate server-side vulnerabilities, reduce operational and deployment costs, and deploy interoperable hardware, software, and biometric authentication solutions. Additionally, OneSpan's single-button Digipass hardware authenticators enable two factor authentication (2FA), support multiple OTPs, and create a unique signature for every transaction.

Analyst Perspective

Following is the analysis of OneSpan's capabilities in the user authentication market:

- OneSpan offers a comprehensive set of robust, frictionless authentication solutions as well as invisible security features to help organizations to achieve their security objectives. OneSpan helps organizations minimize fraud, enhance customer satisfaction, and meet regulatory requirements with its intelligent adaptive authentication. It also enhances security and authentication by gaining visibility into mobile security issues with its mobile security suite. It improves remote access security with two-factor authentication, prevents fraud, and safeguards high-value transactions with user-friendly hardware authentication devices. Additionally, it utilizes authentication server and API technologies to protect access and transactions and streamline identity management.

- In terms of geographical presence, OneSpan has a strong global presence with offices at major locations in the USA, Canada, and Europe. OneSpan has a presence in many industry verticals, including financial services, healthcare, government, and insurance. From a use case perspective, OneSpan offers frictionless authentication, application fraud, regulatory compliance, enterprise security, account takeover, and more.

- OneSpan's key challenges include the growing competition from emerging vendors with innovative technology offerings who tend to serve a certain section of employees. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-sized organizations and are amongst the key targets for mergers and acquisitions. However, with its comprehensive functional capabilities, compelling customer references, and robust customer value proposition, OneSpan is well-positioned to maintain and grow its market share.

- Concerning technology roadmap, OneSpan is investing on increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

Ping Identity

URL: https://www.pingidentity.com

Founded in 2002 and headquartered in Denver, Colorado, Ping Identity is a leading provider of secured identity solutions and services for enterprises globally. The company offers zero-trust identity-defined security to organizations to enhance protection and engagement across global businesses. The PingOne Cloud Platform allows customers, employees, and partners to securely access the cloud, mobile (web), SaaS and on-premise applications and APIs.

The PingOne Cloud Platform enables organizations to build and manage user profiles, validate users' identities, authenticate users using consistent sign-on and multi-factor authentication, secure access to resources, data, and sensitive activities, and constantly monitor risk signals and API traffic. The PingOne Cloud Platform offers an identity verification service titled PingOne Verify that allows customers to easily verify their identities to improve and minimize account creation fraud. In addition, the company provides a machine learning-based Risk Management service named PingOne Risk to protect authentications and provide visibility into organizational threats and other services titled PingOne MFA (multi-factor authentication) to provide a secure and seamless experience to customers and PingID, a multi-factor authentication solution for workforces to optimize security and productivity.

PingOne Cloud Platform leverages open standard-based advanced single sign-on for customers, employees, and partners to authenticate and sign into any application from any device and any device. The PingOne Cloud Platform utilizes advanced access security that centralizes apps and APIs access to URL and HTTP method levels. Additionally, PingOne Advanced Access Security offers a comprehensive policy engine and risk-aware authorization to resources and application-scoped session tokens. PingOne Cloud Platform also offers an advanced directory to securely manage identity and profile data. It also supports unstructured data, and scales to millions of identities and exposes them via APIs, and offers centralized authorization policies with Dynamic Authorization to secure sensitive data and actions. Additionally, Dynamic Authorization provides a drag-and-drop UI that allows anyone to update policies.

PingOne Cloud Platform offers AI-based API security to automate API discovery, deep traffic visibility, reporting, threat detection, and cyberattack prevention. Additionally, PingOne Cloud Platform provides centralized administration, which includes self-service IAM application integration capabilities, as well as a unified operating portal with workflows, templates, orchestration automation, lifecycle management, and central monitoring. PingOne Cloud Platform allows users to secure and control their personal information and seamlessly share valuable and verified data with its Personal identity.

PingOne Cloud Platform leverages artificial intelligence and integrations with different risk, fraud, and threat signals for better authentication decisions. PingOne Cloud Platform

Identity intelligence helps provide secure and simple interactions by syncing, collecting, and safeguarding data from many sources, enforcing authentication, conditional access, and authorization restrictions based on risk. Additionally, it supports passwordless authentication and real-time authorization. The PingOne Cloud Platform also offers comprehensive APIs for integration and customization, as well as a turnkey integration kit to quickly connect with organizational SaaS, web, mobile, and traditional apps.

PingOne Cloud Platform offers multiple self-service capabilities to administrators, developers, and users to control their identities and customer experiences at the enterprise level. Additionally, the platform allows administrators to control admin-specific product and environment configurations through a unified operating portal. It also allows developers to integrate identity services into their apps and users to create new accounts, manage profiles, and secure their data. The company supports multiple deployment options for its platform, including cloud (IDaaS), private cloud, or as an on-premise software solution.

Analyst Perspective

Followings are the analysis of Ping Identity's capabilities in the global User Authentication market:

- Ping Identity offers a comprehensive and standards-based platform titled PingOne Cloud Platform for hybrid, multi-generational, and multi-cloud environments. The platform allows workforce, customer, and partner identities to securely access any services, applications, or API from any device. The solution offers global authentication, a secure and seamless user interface for business initiatives, and comprehensive APIs for integration and customization.

- Some of the key differentiating features of the PingOne Cloud Platform include proven scalability and performance for some of the world's largest and most dependable CAIM implementations, hybrid and multi-cloud deployments, standard protocol support for legacy and modern access management use cases, market-leading multifactor authentication, risk management and authentication services, PingOne Verify with Identity Verification, and PingOne for Individuals for Personal Identity. Additionally, it supports standards protocols through OOTB integration with Microsoft O365, social identity providers, token translators, OAUTH/OIDC, SCIM, and more.

- Concerning geographical presence, Ping Identity has a very strong presence in North America. The company also has a significant presence in Europe and the Asia Pacific. From the industry vertical perspective, the company has a presence across a wide variety of industry verticals, including banking, and financial services, followed by healthcare, IT, software, telecom, and retail. From the use case perspective, Ping Identity supports employee and partner solutions,

customer solutions, modernizing legacy IAM, passwordless authentication, zero trust, and mitigate fraud risk.

- The primary challenges for Ping Identity include the growing competition from emerging vendors with innovative technology offerings. These vendors have successfully gained a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its sophisticated technology platform, comprehensive functional capabilities, robust roadmap, compelling customer references, and customer value proposition, Ping Identity is well-positioned to maintain and grow its share in the User Authentication market.

- Concerning technology roadmap, Ping Identity is investing in ID verification & digital credentialing services, orchestration, dynamic authorization as a service-Cloud-hybrid Externalized Authorization Management (EAM) and launch the PingOne marketplace. From a long-term roadmap perspective, the company is investing in PingOne Fraud (SecuredTouch), personal identity platform, personal identity standards, decentralized identity foundation, W3C, and OIDF. Additionally, the company is focusing on implementing a centralized business intelligence and analytics program to serve all functions internally at Ping and integrate the PingOne product data with CRM data to generate insights across the entire customer cloud experience.

Prove

URL: https://www.prove.com

Founded in 2015 and headquartered in Redwood City, California, US, UnifyID has been acquired by Prove in 2021. Prove offers a next-generation Identity-verification software to protect from identity theft and social engineering attacks by identifying individuals with just a phone. Prove provides multi-factor authentication services which leverage deterministic biometric and environmental attributes using machine learning to detect users. Prove allows organizations to authenticate users with its GaitAuth. Prove's GaitAuth enables organizations to passively authenticate users based on their gait (unique walking style).

Prove's GaitAuth provides secure passive authentication and combines individual manner of walking with proprietary machine-learning algorithms to provide authentication without user intervention. Additionally, Prove GaitAuth operates with step-up or continuous authentication routines, as well as a factor in a 2FA/MFA solution. The Prove GaitAuth SDK offers simple APIs to integrate passive gait-based authentication into users' mobile applications by integrating the GaitAuth SDK into the user's app, creating and training models for users, and leveraging gate fracture scores from trained models in users' apps authentication flow. Additionally, the product allows organizations to identify whether the user of the phone is who they claim to be or an attacker with its machine learning-based mobile SDK.

Prove's GaitAuth allows organizations to correctly detect users with accuracy revealing the same as other biometric authentication methods, minimize the explicit authentication methods, continuously authenticate users without interrupting, and differentiate themselves from the competitors with passive authentication. Additionally, Prove's GaitAuth supports Android apps and IFTTT rules. Prove also allows users to improve push notification capabilities by leveraging contextual behavioral signals.

Analyst Perspective

Followings are the analysis of Prove's capabilities in the global User Authentication market:

- Prove offers a motion behavioral biometric-based authentication solution titled GaitAuth, which leverages motion sensors on users' phones to provide user authentication. The solution can also combine with desktops. Some of the key differentiators of the company include motion-based behavioral biometrics based on gait, support for cross-channel authentication, runs in the background, false positive rate of 1,50,000, and providing contextual information from a few moments before and after the authentication request.

- Concerning geographical presence, Prove has a strong presence in the US and Canada followed by Europe, Asia Pacific, and Latin America. From the industry vertical perspective, the company has a presence across a wide variety of industry

verticals, including banking & financial services, IT & Telecom, retail & eCommerce, govt & public sectors, healthcare & life sciences, and such others. From a use case perspective, Prove supports push authentication, behavioral biometrics, replacement 2FA, physical access, and promotion fraud detection.

- The primary challenges before Prove include the growing competition from emerging vendors with innovative technology offerings. These vendors have successfully gained a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. Additionally, the company might face some challenges in expanding its presence across Canada, and Middle East & Africa markets due to the growing competition from other well-established players. However, with its sophisticated technology platform, comprehensive functional capabilities, robust roadmap, compelling customer references, and customer value proposition, Prove is well-positioned to maintain and grow its market share in the User Authentication market.
- Concerning technology roadmap, Prove is investing in contextual signals and model improvements. Additionally, the company is focusing on increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

Thales

URL: https://www.thalesgroup.com

Founded in 2000 and headquartered in Austin, Texas, US, Thales is a provider of solutions for the defense, aeronautics, space, and digital identity and security domains. Thales offers a robust identity authentication and authentication portfolio through its SafeNet Trusted Access. The data protection and cyber security solution helps organizations minimize risks, verify compliance, and improve flexibility. SafeNet Trusted Access provides trusted access and offers comprehensive capabilities to protect the cloud and data from various types of threats.

Thales SafeNet Trusted Access provides cloud and web single sign-on (SSO) with granular access security, which allows organizations to secure and provide quick access to different cloud applications by validating identities and implementing access policies. Additionally, the Thales SSO helps organizations eliminate password fatigue, frustration, and password resets, Thales SafeNet Trusted Access supports numerous authentication methods and allows organizations to leverage authentication schemes already deployed in the organization. Additionally, the solution helps to improve user ease and manage risk context-based authentication.

Thales SafeNet Trusted Access offers flexible access management via an easy-to-use policy engine, which provides real-time control over the capacity to enforce policies at the individual user, group, or application level. Additionally, the solution supports existing authentication techniques to protect cloud and web-based services. Thales SafeNet Trusted Access supports different authentication methods, including context-based authentication combined with step-up capabilities, OOB, one-time password (OTP), and X.509 certificate-based solutions. Additionally, all the authentication methods are provided through smart cards, USB tokens, software, mobile app, and hardware tokens. Additionally, Thales SafeNet Trusted Access offers certificate-based PKI USB authentication tokens, certificate-based smart cards, FIDO devices, OTP authenticators, tokenless authenticators, and passwordless authentication to protect the cloud, data, and trusted access.

Thales' SafeNet PKI USB authentication tokens and certificate-based smart cards provide strong multi-factor authentication, which allows organizations to meet their PKI security needs. Thales SafeNet PKI USB and certificate-based smart cards offer a unified solution for authentication and application access control, including remote access, network access, password management, network login, sophisticated applications such as digital signature and data and email encryption and corporate ID badges, magnetic stripes, and proximity. Thales' SafeNet USB authentication tokens include SafeNet e Token 5110 and SafeNet e Token 5300. Thales's SafeNet Trusted Access includes SafeNet IDPrime Smart Cards, SafeNet IDPrime PIV Smart Cards, SafeNet IDCore Smart Cards, SafeNet Authentication Client, and SafeNet Minidriver. Thales's SafeNet Trusted Access FIDO card and the FIDO token enable organizations to protect cloud adoption and bridge secure

access across hybrid environments via integrated access management and authentication offering.

Thales's SafeNet Trusted Access includes FIDO and FIDO2 devices, which enable organizations to create a seamless and passwordless login experience. Thales SafeNet Trusted Access utilizes tokenless authentication solutions, including out-of-band or SMS, push OTP, software authentication, and grid or pattern-based authentication to protect users from hacking and data breaches.

Analyst Perspective

Followings are the analysis of Thales capabilities in the global User Authentication market:

- Thales offers a cloud-based access management solution titled SafeNet Trusted Access, which helps organizations control access to both cloud services and business applications through an integrated platform that combines single sign-on, multi-factor authentication, and scenario-based access regulations. Additionally, the solution enables organizations to enhance the adoption of cloud services for end-users who face challenges in managing online identities and access security while ensuring comfortability and regulatory compliance.

- SafeNet Trusted Access provides centralized user access control, enhanced security through fine-grained access policies, visibility into all access for simplified compliance, secured access to partners and contractors, fast and easy cloud access through Smart Single Sign-On, and efficiency of identity-as-a-service. Additionally, it automates cloud identity management and enables IT support and users to minimize password hassles while delivering a single pane view of access activities throughout the organizational app to verify that the correct user has access to the right application at the right level of confidence.

- Concerning geographical presence, Thales has a strong presence in the US and Europe, followed by the Asia Pacific and the Middle East and Africa. From the industry vertical perspective, the company has a presence across a wide variety of industry verticals, including healthcare, manufacturing, electric utilities, energy, education, financial services, government, retail, sports and entertainment, and media & entertainment. From a use case perspective, Thales supports secure remote access, secure VPN access, VDI security solutions, secure cloud access, 2FA solutions, web and cloud SSO, and physical & logical access control.

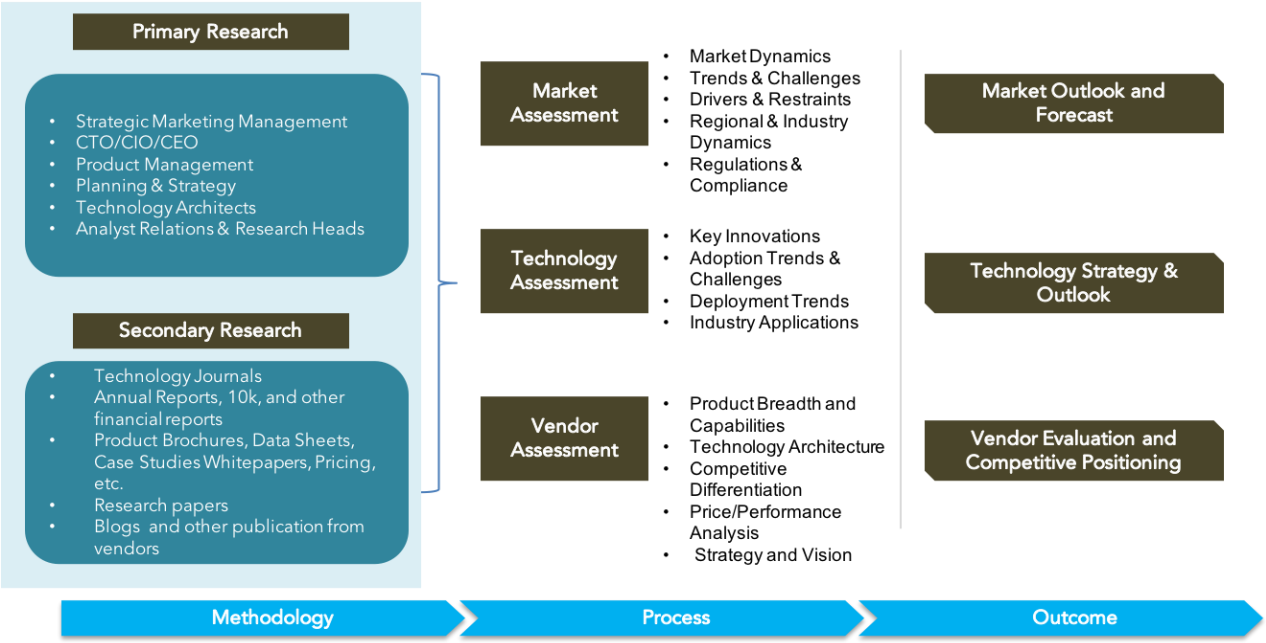
- Thales’s primary challenges include the growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value

proposition, Thales is well-positioned to maintain and grow its market share in the User Authentication market.

- Concerning technology roadmap, Thales is focusing on enhancing user authentication capabilities, increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

Research Methodologies

Quadrant Knowledge Solutions uses a comprehensive approach to conduct global market outlook research for various technologies. Quadrant's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. Following is a brief description of the major sections of our research methodologies.



Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant's Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists
- Published secondary data on companies and their products
- Database of market sizes and forecast data for different market segments
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

Quadrant analysts collect relevant documents such as whitepapers, brochures, case studies, price lists, datasheet, and other reports from all major industry participants.

Primary Research

Quadrant analysts use a two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The Quadrant research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: Quadrant analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analysts also get their first-hand experience with the vendor's product demo to understand their technology capabilities, user experiences, product features, and other aspects. Based on the requirements, Quadrant analysts interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

Quadrant research team research with various sales channel partners, including distributors, system integrators, and consultants to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

Data Analysis: Market Forecast & Competition Analysis

Quadrant's analysts' team gathers all the necessary information from secondary research and primary research to a computer database. These databases are then analyzed, verified, and cross-tabulated in numerous ways to get the right picture of the overall market and its segments. After analyzing all the market data, industry trends, market trends, technology trends, and key issues, we prepare preliminary market forecasts. This preliminary market forecast is tested against several market scenarios, economic scenario, industry trends, and economic dynamics. Finally, the analyst team arrives at the most accurate forecast scenario for the overall market and its segments.

In addition to market forecasts, our team conducts a detailed review of industry participants to prepare competitive landscape and market positioning analysis for the overall market as well as for various market segments.

SPARK Matrix: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After finalization of market analysis and forecasts, our analyst prepares necessary graphs, charts, and table to get further insights and preparation of the final research report. Our final research report includes information including market forecast; competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.